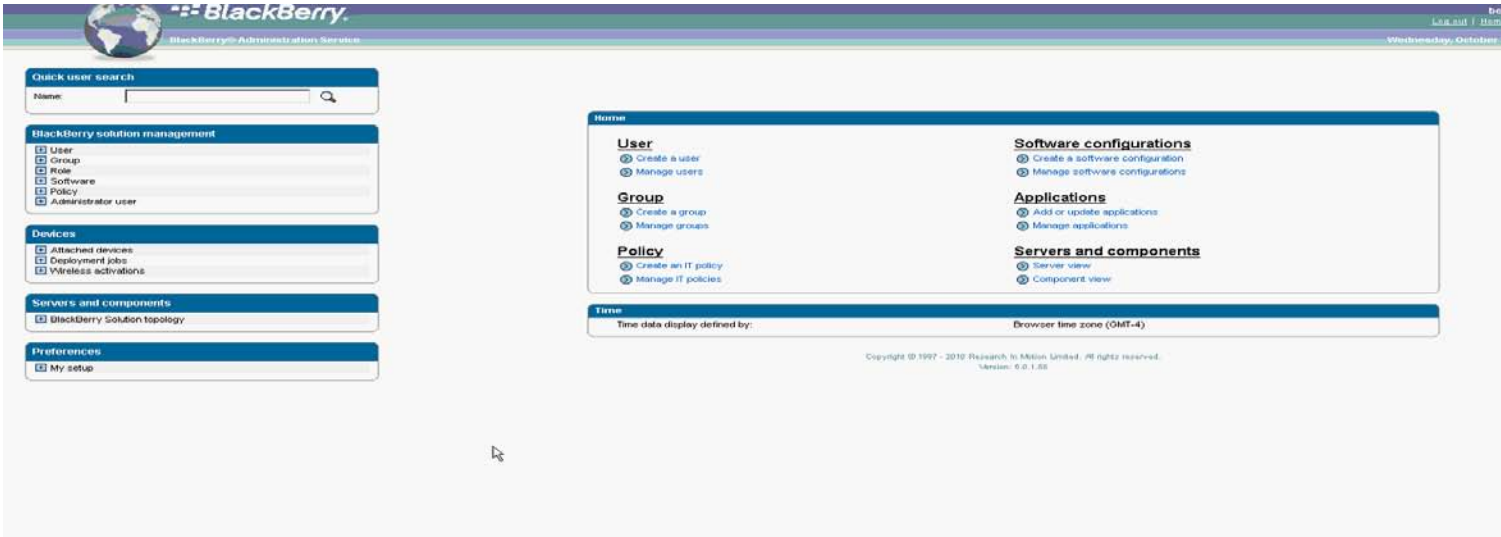
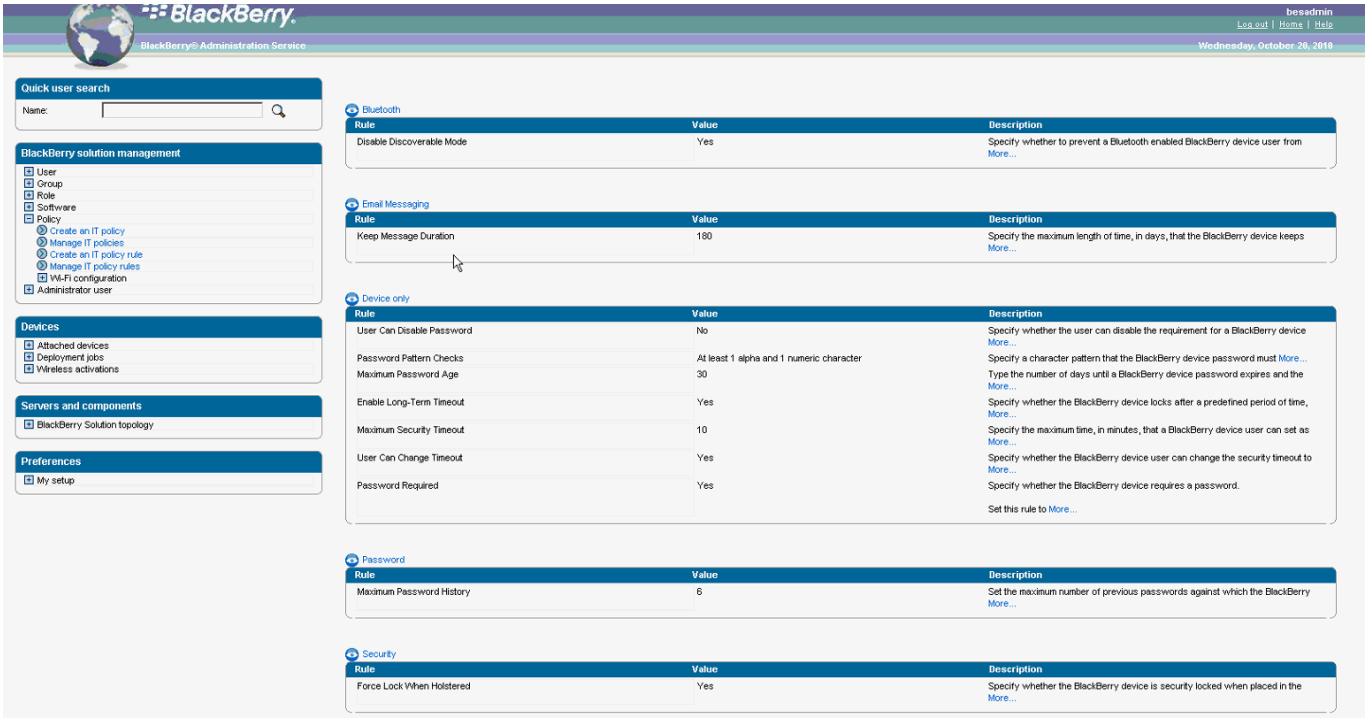
BlackBerry Devices and their policies are managed by a BlackBerry Enterprise Server (BES). IT Policies contain all the settings and preferences that are downloaded to the BlackBerry device. When a PGP Universal Server is deployed, the BlackBerry devices do not communicate to the PGP Universal Server, but rather the BES communicates with the PGP Universal Server. The BlackBerry devices receive PGP Universal Server policy via the BES.

The user interface of the BlackBerry Enterprise Server (BES).



The figure below shows a basic IT Policy on a BES 5.0 server. One big difference from BES 4.x to the BES 5.0 server, is the usage of a web interface by the BES 5.0 server.

The BES supports multiple IT Policies, and the BlackBerry devices are assigned to a policy once the device completes the Enterprise Activation process.


BlackBerry.
BlackBerry® Administration Service
besadmin
Log out | Home | Help
Wednesday, October 20, 2010
Quick user search
Name:
BlackBerry solution management
User
Group
Role
Software
Policy
Create an IT policy
Manage IT policies
Create an IT policy rule
Manage IT policy rules
Wi-Fi configuration
Administrator user
Devices
Attached devices
Deployment jobs
Wireless activations
Servers and components
BlackBerry Solution topology
Preferences
My setup
Bluetooth
Rule | Value | Description
Disable Discoverable Mode | Yes | Specify whether to prevent a Bluetooth enabled BlackBerry device user from More...
Email Messaging
Rule | Value | Description
Keep Message Duration | 180 | Specify the maximum length of time, in days, that the BlackBerry device keeps More...
Device only
Rule | Value | Description
User Can Disable Password | No | Specify whether the user can disable the requirement for a BlackBerry device More...
Password Pattern Checks | At least 1 alpha and 1 numeric character | Specify a character pattern that the BlackBerry device password must More...
Maximum Password Age | 30 | Type the number of days until a BlackBerry device password expires and the More...
Enable Long-Term Timeout | Yes | Specify whether the BlackBerry device locks after a predefined period of time, More...
Maximum Security Timeout | 10 | Specify the maximum time, in minutes, that a BlackBerry device user can set as More...
User Can Change Timeout | Yes | Specify whether the BlackBerry device user can change the security timeout to More...
Password Required | Yes | Specify whether the BlackBerry device requires a password. Set this rule to More...
Password
Rule | Value | Description
Maximum Password History | 6 | Set the maximum number of previous passwords against which the BlackBerry More...
Security
Rule | Value | Description
Force Lock When Holstered | Yes | Specify whether the BlackBerry device is security locked when placed in the More...

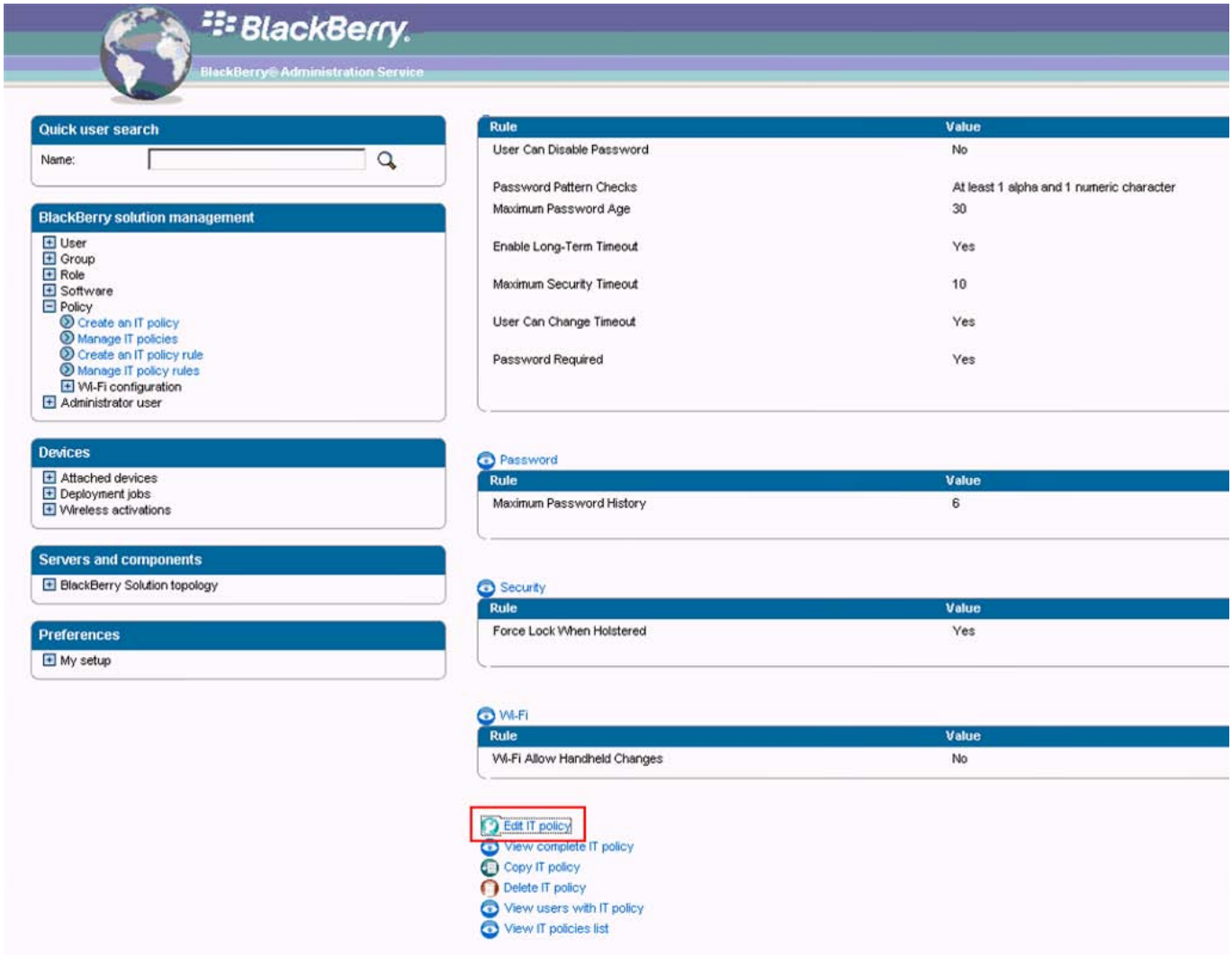
Once a BlackBerry device completes the Enterprise Activation process, ensure the device shows up under the correct BES IT policy.

To see which IT Policy the BlackBerry device is assigned to:

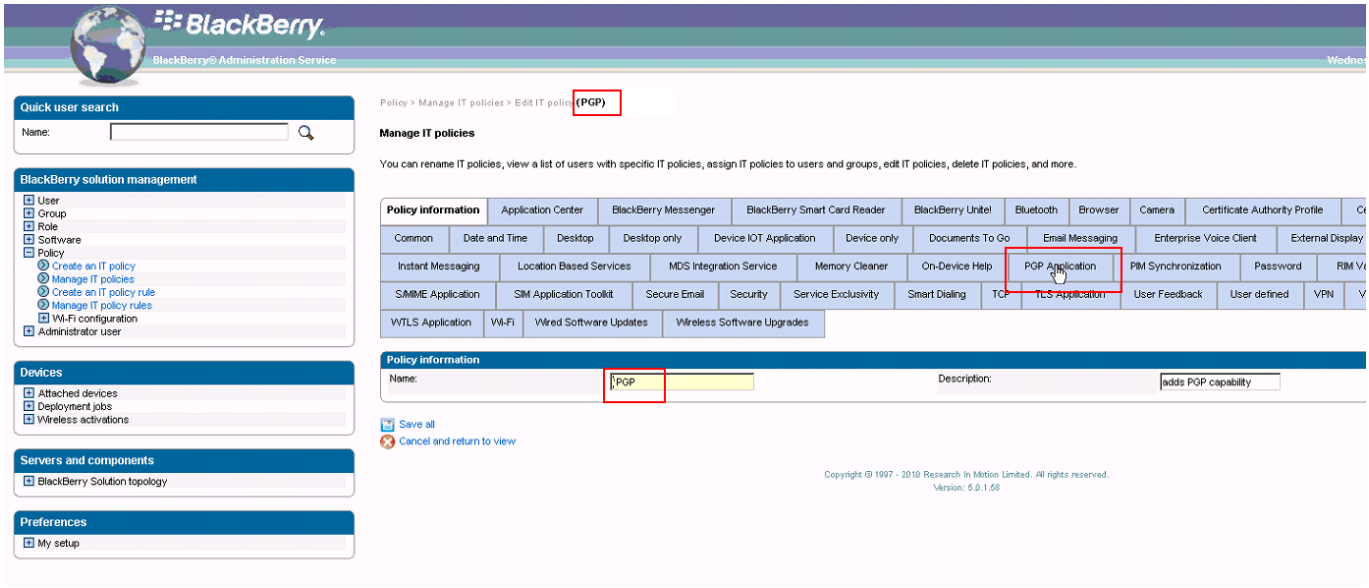
1. On the BES, open **Options** on the BlackBerry device.
2. Go to **Security Options > General Settings** and scroll down the list of general settings to “IT Policy Name”.

This lists the name of the policy the device is managed by the BES. Check the BES to ensure this is the expected policy.

Once the BlackBerry device is confirmed to be in the correct IT Policy on the BES, a policy for PGP can be created by clicking **Edit IT Policy**.

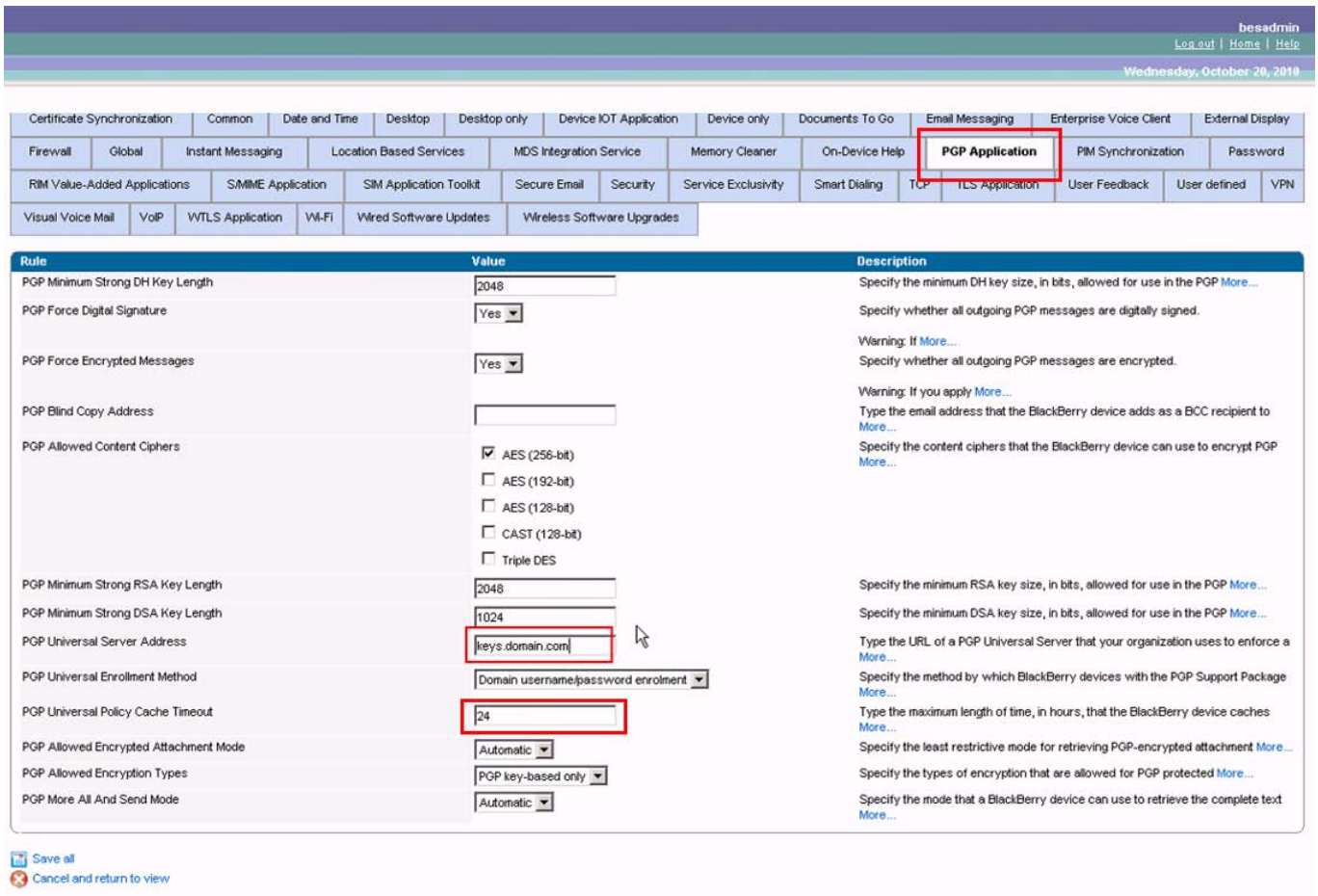


This opens a window to add the desired policy. In this example, the new BES IT Policy is “PGP”:



Click the PGP Application tab to add PGP functionality to the BES IT Policy.

The following image displays the PGP features that can be integrated with BlackBerry devices. Review all the fields as per the user's guide to understand which option is best for you. In this example, the name of the PGP Universal Server is called *keys.domain.com*. The BES must be able to resolve the hostname (FQDN) of the PGP Universal Server and communicate with server over port 443.


besadmin
Log out | Home | Help
Wednesday, October 20, 2010
Certificate Synchronization
Common
Date and Time
Desktop
Desktop only
Device IOT Application
Device only
Documents To Go
Email Messaging
Enterprise Voice Client
External Display
Firewall
Global
Instant Messaging
Location Based Services
MDS Integration Service
Memory Cleaner
On-Device Help
PGP Application
PIM Synchronization
Password
RIM Value-Added Applications
S/MIME Application
SIM Application Toolkit
Secure Email
Security
Service Exclusivity
Smart Dialing
TCP
TLS Application
User Feedback
User defined
VPN
Visual Voice Mail
VoIP
WTLS Application
Wi-Fi
Wired Software Updates
Wireless Software Upgrades
Rule
Value
Description
PGP Minimum Strong DH Key Length
2048
Specify the minimum DH key size, in bits, allowed for use in the PGP More...
PGP Force Digital Signature
Yes
Specify whether all outgoing PGP messages are digitally signed.
Warning: If More...
PGP Force Encrypted Messages
Yes
Specify whether all outgoing PGP messages are encrypted.
Warning: If you apply More...
PGP Blind Copy Address
Type the email address that the BlackBerry device adds as a BCC recipient to More...
PGP Allowed Content Ciphers
AES (256-bit)
AES (192-bit)
AES (128-bit)
CAST (128-bit)
Triple DES
Specify the content ciphers that the BlackBerry device can use to encrypt PGP More...
PGP Minimum Strong RSA Key Length
2048
Specify the minimum RSA key size, in bits, allowed for use in the PGP More...
PGP Minimum Strong DSA Key Length
1024
Specify the minimum DSA key size, in bits, allowed for use in the PGP More...
PGP Universal Server Address
keys.domain.com
Type the URL of a PGP Universal Server that your organization uses to enforce a More...
PGP Universal Enrollment Method
Domain username/password enrolment
Specify the method by which BlackBerry devices with the PGP Support Package More...
PGP Universal Policy Cache Timeout
24
Type the maximum length of time, in hours, that the BlackBerry device caches More...
PGP Allowed Encrypted Attachment Mode
Automatic
Specify the least restrictive mode for retrieving PGP-encrypted attachment More...
PGP Allowed Encryption Types
PGP key-based only
Specify the types of encryption that are allowed for PGP protected More...
PGP More All And Send Mode
Automatic
Specify the mode that a BlackBerry device can use to retrieve the complete text More...
Save all
Cancel and return to view

Once the policy is configured, click the **Save All** button to save the changes.

In the preceding example, we have chosen the enrollment method of entering a domain password. This is probably the easiest option as it immediately authenticates the user for PGP enrollment using the users domain credentials.

Once the changes are made, it is necessary to resynchronize the BES IT Policy on the BlackBerry device. One method to force the IT Policy synchronization is to turn off the device and pull the battery. The rebooting of the device will force IT Policy to be downloaded from the BES server.

Now the BES should be ready to manage BlackBerry devices with the PGP Universal Server.

To enroll a user on a BlackBerry device, a user account must exist on the PGP Universal Server. If the PGP Universal Server is configured to use *Directory Synchronization* to query users in a domain LDAP directory such as Active Directory, the user being enrolled must also be present in the LDAP directory.

Once the BES has been configured, the PGP Universal Server must be configured.

PGP Policies on the BES:

PGP Universal Policy Cache Timeout

- One notable entry in the PGP policy on the BES is the “PGP Universal Cache Timeout” This setting is how often the BlackBerry device is going to request policy from the BES for PGP information such as PGP keys for recipients.

- The default is 24 hours and the max is 48 hours. This means that every 24-48 hours, when sending a message, the BlackBerry will need to get policy from the BES once again, which can take extra time (possibly 10 seconds per new recipient per new synchronization, even w/out encrypting the message).

- Depending on the customer needs, this may need to be adjusted to 48hrs to reduce the occurrence of this prompt on the BlackBerry device.

PGP Force Encrypted Messages

PGP Force Encrypted Messages IT Policy rule that has been changed since BES version 4.x for the PGP Universal policy.

There are three options available for this setting and each option has a different behavior. Below is the behavior we would expect:

- Default Value is “NO”.
- Blank= Gives the user flexibility to send encrypted or not.
- Based on our testing in support, it shows the device still follows mail policy on Universal Server, even if plain text is selected for encoding. If a rule on Universal Server is set to never encrypt, this will be enforced and the message will be sent in the clear. If the encoding “Encrypt” is selected on the BlackBerry device, the device will in fact attempt to encrypt a message, thus defaulting to a higher security option, even if the Universal Server says send unencrypted.
- No=Does not allow encryption, never sends encrypted in any case and ignores any Universal Server policy.
- Yes=Forces encryption regardless of PGP Universal Policy, if it can’t encrypt the message, it can’t send the message.

Getting started with the PGP Support Package

The following KB articles include more information:

1. Where can the latest BlackBerry device software be found:
Article URL http://www.symantec.com/docs/TECH149101

2. Installing the PGP Support Package (via Device Manager):
Article URL http://www.symantec.com/docs/TECH148931

3. Installing the PGP Support Package Over The Air (OTA via the BES):
Article URL http://www.symantec.com/docs/HOWTO42045